JPIP より得られる JPEG 2000 画像に適した画像認証システム

小出　雅史 †　　岩村　惠市 †

† 東京理科大学
102-0073 東京都千代田区九段北 1-14-6

koide@sec.ee.kagu.tus.ac.jp

あらまし　JPEG 2000 画像の通信プロトコルである JPIP より得られた画像への著作権の主張を可能とする画像認証システムを提案する．JPIP では，ユーザが必要とする JPEG 2000 画像データだけを送信することで，各ユーザは要求した JPEG 2000 画像を入手できる．JPEG 画像などは圧縮後のデータ構成は固定され，ユーザはその画像データを復号する．よって，その画像に対して著作権の主張を考えた場合，RSA 署名や ECDSA 署名を用いてその主張が可能である．しかし，ユーザが JPIP より JPEG 2000 画像を得た場合，その JPEG 2000 画像のデータ構成はユーザの要求によって異なってしまう．すなわち，JPIP より得られた JPEG 2000 画像は従来の署名技術を用いて著作権の主張を可能とすることが難しい．本稿では Boneh らによる Aggregate 署名を用いて，JPIP より得られた JPEG 2000 画像への著作権の主張を可能とする画像認証方式を示す．

An Image Authentication System Suitable For JPEG 2000

Masafumi Koide†　　Keiichi Iwamura†

†Tokyo University of Science
1-14-6 Kudankita Chiyoda-ku Tokyo 102-0073 Japan

koide@sec.ee.kagu.tus.ac.jp

Abstract　In this paper, we propose an image authentication system for JPEG 2000 images that are obtained by the JPEG 2000 Interactive Protocol (JPIP). Digital signature is one of the image authentication tools. It can be applied to digital image with a fixed codestream structure, such as a JPEG image. However, the JPIP permits a user to select decoding data that is a portion of a JPEG 2000 codestream. Thus, a JPEG 2000 image codestream, which a user obtained using JPIP, varies its structure according to his/her requests. Therefore, a JPEG 2000 images obtained by JPIP cannot be authenticated using a conventional digital signature such as RSA, DSA, etc. To solve this problem, we adapted an aggregate signature to the JPEG 2000 images. The aggregate signature is a digital signature that some signatures are aggregated into but requires only one verification. We show the concrete authentication system for the JPEG 2000 image obtained by JPIP using the aggregate signature.

1　はじめに

画像認証で用いられる技術としては，電子透かしやデジタル署名が挙げられる．画像認証に関する研究としては，電子透かしを用いたものが一般的である．しかし，電子透かしの埋め込み方法のアルゴリズムは公開できないものが多い．その理由としては，電子透かしはアルゴリ

ズムを公開した場合，攻撃への耐性が低くなることが挙げられる．

そこで，本稿ではアルゴリズムが公開されており，安全性の根拠を数学的問題に帰着したデジタル署名を認証技術として用いることにした．デジタル署名とは，捺印やサインに相当する機能をデジタルデータに対して実現するための技術である．この技術により，コンテンツの改ざんや著作者へのなりすましを防止することができ，デジタルコンテンツの保護を実現することができる．そこで，このデジタル署名を用いて，JPEG 画像と画像符号化方式の新しい国際標準である JPEG 2000 [1] への認証方式を検討する．

初めに，JPEG 画像への認証は RSA 署名や ECDSA 署名などにより可能である．JPEG 画像は圧縮後のデータ構成は固定され，ユーザはその画像データを復号する．よって，その画像に対する認証システムを考えた場合，RSA 署名や ECDSA 署名を用いて著作者が署名を施すことでその主張が可能である．

しかし，JPEG 2000 画像に対しては JPEG 画像と同様に著作権保護を検討することができない．JPEG 2000 は，1 度符号化された画像に対しても復号側が色空間・解像度等を選択することによって表現の異なる画像を構成することを可能としている．そして，JPEG 2000 の通信プロトコルとして JPIP [2,3] というものがある．JPIP ではユーザとサーバ間で通信が行わる．そこでは，サーバがユーザの要求に応じて，保存されている JPEG 2000 画像符号列を再構成して送信する．つまり，JPIP により送信される画像データの構成はユーザごとに異なってしまう．

ここで，JPIP より得られた JPEG 2000 画像に対する認証システムを JPEG 画像の認証方式と同様に検討する．初めに，著作者が自分の JPEG 2000 画像データ全体に対してデジタル署名を生成し，その画像データと署名をサーバに保管している場合を考える．次に，ユーザが JPIP より要求した画像を得て，その画像の正当性を検証したいとする．しかし，ユーザが得た画像はサーバ上のデータを再構成したものであるから，サーバに保存してある全体からのデジタル署名では検証することが出来ないという問題がある．よって，JPIP により得られた JPEG 2000 画像では著作権を保護するために，従来のデジタル署名を用いた検証ができない．これらの問題をふまえて，提案方式では受信された再構成コンテンツが著作者のオリジナルコンテンツデータの一部であることと，その改ざん検出が同時に実現できるようにする．

本稿では，Boneh らによって提案された Aggregate 署名 [4] を用いることで，JPIP より得られる JPEG 2000 画像へのデジタル署名の適応を考える．Aggregate 署名とは複数のデータに対して個別に署名を生成し，それらを一つに集約した署名のことである．また，検証者はその一つの Aggregate 署名の検証を通じて全ての個別署名を検証することができる．JPEG 2000 の符号列は，Packet と呼ばれる最小単位の符号列（byte 単位）で構成されている．そして，JPIP の通信方式にはタイルパート単位とプレシンクト単位の 2 種類の送信方式がある．このどちらかの単位でデータが転送されるのだが，符号列の最小単位は Packet であり，例えどちらの単位で転送されても Packet が要求画像に応じて送信されると考えられる．そこで，この Packet に注目し Packet ごとに個別署名を取ることで，JPIP より得られた画像への認証システムを実現する．

以下，JPEG 2000，JPIP と Aggregate 署名についての説明を 2 章でおこなう．3 章では JPIP より得られた JPEG 2000 画像に適した署名方式を提案する．

2 JPEG 2000

2.1 JPEG 2000 符号列

JPEG 2000 は高い圧縮性能と既存の JPEG にはない豊富な機能を実現することを狙いとして開発された．その JPEG 2000 の特徴であるスケーラビリティの実現には，ウェーブレット変換を行った後に生成される Packet が大きく関わっている．

Packet は JPEG 2000 の符号列における最小単位の領域であり，JPEG 2000 の符号列はこ

の Packet より構成されている．また，JPEG 2000 では符号化処理時に空間的な領域が定義され，その領域にはタイルやプレシンクトがある．そして，Packet データはタイルあるいはプレシンクトの単位から生成される．

2.2 JPIP

JPIP とはサーバとユーザとの間で，JPEG 2000 画像のデータを通信するプロトコルである．JPIP 通信では，ユーザは JPEG 2000 へ圧縮された画像ファイル全てへアクセスすることを必要とせず，必要とする画像領域だけを受けとることが可能である．

ユーザは画像領域，画像のコンポーネント，必要とする解像度レベルなどの情報を決定し，それらをサーバに要求する．そして，サーバはユーザの要求にあった Packet データをタイルまたはプレシンクト領域で結合することで，ユーザが必要とする画像に適した符号列を生成する．

また，JPIP では JPEG 2000 符号列を送信する方式が 2 種類ある．それはタイル領域で送信する JPT-stream とプレシンクト領域で送信する JPP-stream であり，JPIP のメディア方式に適した通信方式である．その方式のどちらにしても，ユーザの要求画像にあった Packet データを選ぶことにより，その画像に対する符号列が構成される．

3 Aggregate 署名

本稿では，デジタル署名を認証手段として用いる．ここでは，デジタル署名の 1 つである Aggregate 署名 [4,5] を説明する．この署名方式は複数の署名者が確かに署名を施したことを検証することを目的として提案されている．本提案方式では，署名を施すのは著作者のみである．Boneh らの方式では，鍵ペアが 1 つ，つまり一人の署名者が複数のメッセージに対して署名を施す場合の検証方法も紹介されている．その概要を以下に示す．

G_1，G_2，G_T を位数 p(素数) の乗法群とし，g_1，g_2 を G_1，G_2 の生成元とする．また，$e : G_1$

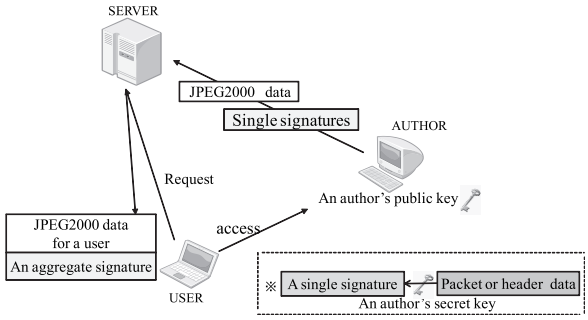

図 1: JPEG 2000 画像への認証システム

$\times G_2 \to G_T$ を双線形写像とする．さらに，ハッシュ関数 $H : \{0,1\} \to G_1$ を定める．Boneh らの Aggregate 署名は以下の 4 つのアルゴリズム KeyGeneration，Sign，Aggregation，AggregateVerification から構成される．ここでは，特別な場合として，1 人の署名者が n 個のメッセージに対して Aggregate 署名の生成，検証の手順を示す．

1. KeyGeneration:
   乱数 $x \in G_1$ に対して，$v \leftarrow g_2^x (v \in G_2)$ を求める．秘密鍵を x，公開鍵を v とする．

2. Sign:
   メッセージ $M_i (i = 1, \ldots, n)$ のそれぞれに対して，$h_i \leftarrow H(M_i)$ を計算し，$\sigma_i \leftarrow {h_i}^x$ を求め，個別署名 $\sigma_i \in G_1$ を出力する．

3. Aggregation:
   個別署名 $\sigma_1, \ldots, \sigma_n \in G_1$ に対して $\sigma = \prod_{i=1}^{n} \sigma_i$ を求め，Aggregate 署名 $\sigma \in G_1$ を出力する．

4. AggregateVerification:
   メッセージ $M_1, \ldots, M_n \in \{0,1\}^*$，公開鍵 $v \in G_2$，Aggregate 署名 $\sigma \in G_1$ に対し，$e(\sigma, g_2) = e\left(\prod_{i=1}^{n} H(M_i), v\right)$ が成り立つかを検証する．

Aggregate 署名の安全性は，群ペア (G_1, G_2) における co-CDH 問題は困難であるという仮定に基づく．群ペア (G_1, G_2) における co-CDH 問題とは，$g, g^a \in G_1$，$h \in G_2$ から $h^a \in G_2$ を求める問題である．

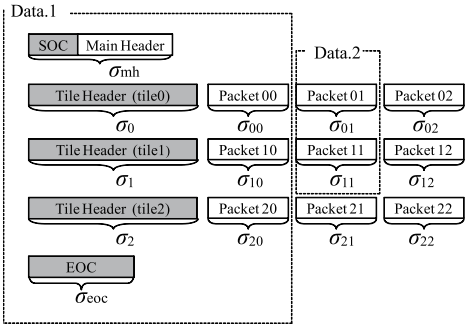

図 2: JPEG 2000 符号列と個別署名

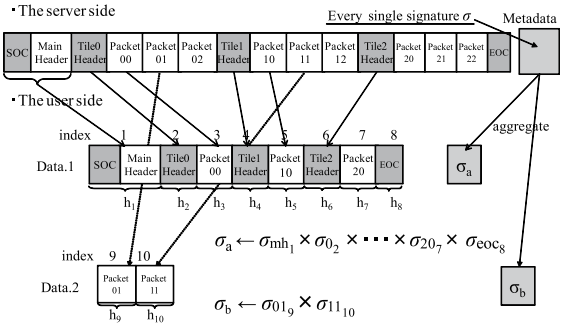

図 3: 個別署名の集約処理例

4 JPEG 2000 画像認証システム

4.1 JPEG 2000 画像への署名方法

Boneh らによる Aggregate 署名での鍵生成は，各ユーザに対して鍵ペアを与えていたが，提案方式では著作者の鍵ペアだけを生成する．そして，著作者は各 Packet に対して個別署名を生成し，それらをサーバに保存する．

JPIP は前述したように，要求に応じて JPEG 2000 データを転送する．ここで注目すべきは JPEG 2000 データを構成する最小単位は Packet であるということである．そして，JPIP では要求画像に必要なデータに該当する Packet を選んで送信していると考えることができる．よって，各 Packet に対して署名を取り，それを個別署名としてサーバに保存することにした．なお，各 Header に対しても個別署名を生成する．

4.2 JPEG 2000 画像への認証システム

初めに，前提条件をまとめる．

- コンテンツの著作者は有効な署名鍵を持っている．
- コンテンツの著作者をユーザは知っている．

次に提案方式の概要について述べる．図 1 に提案方式の概要を示す．著作者は自分の秘密鍵で個別署名を生成し，サーバに JPEG 2000 データと個別署名を保存する．JPIP 通信により画像データを転送する際に，サーバはユーザが要求したデータに該当する個別署名に番号を振り分け，それらを集約し，1 つの Aggregate 署名を生成する．

その後，画像データと生成された Aggregate 署名を送信する．なお，その Aggregate 署名はその画像データの正当性を保証するものである．このとき，この Aggregate 署名はメタデータとして送信され，ユーザ側で画像データと共に保存される．検証は，ユーザが得た画像データ，著作者の公開鍵とユーザへ送信された Aggregate 署名の 3 つのデータを用いることで行われ，各通信時に行う．

また，最初の通信が終了したとき，ユーザは受け取っている Aggregate 署名を更に集約して，それを最終的な Aggregate 署名としてもう 1 度検証を行う．検証が成功すれば，ユーザが得た画像データは確かに著作者のオリジナルコンテンツであり，著作者が確かに作成した画像であることが確認できる．

さらに提案方式の一例として，図 2 のように Data.1 と Data.2 が 2 回に分けられて送信される場合について説明を加える．なお，Data.1 は 1 回目の通信でおくられたアイコン画像であり，Data.2 は 1 回目の通信で送られた画像の解像度を上げるものとする．また，図 2 のようなデータを送る場合の JPIP ストリームが構成されるときにおける署名の集約方法とその Aggregate 署名を図 3 に示す．

- Key Generation.
  乱数 $x \in G_1$ に対して，$v \leftarrow g_2^x$ $(v \in G_2)$ を求める．この JPEG 2000 画像の著作者の鍵ペアを秘密鍵 x，公開鍵 v とする．

- Signing.
  著作者：$h_n \leftarrow H(\text{Header } n)$，$h_{nm} \leftarrow H(\text{Packet } nm)$ を計算する．そして，個別署名 $\sigma_n \leftarrow {h_n}^x$，$\sigma_{nm} \leftarrow (h_{nm})^x$ を出力し，サーバへ保存する．それぞれの個別署名は σ_n,$\sigma_{nm} \in G_1$ である．

- 最初の通信時.
  サーバ側: 送信されるそれぞれの署名と各データに対して同じ番号を割り振る．そして送信されるデータに該当する個別署名を集約し，Aggregate 署名 σ_a を生成する．($\sigma_a \leftarrow \sigma_{mh_1} \times \sigma_{0_2} \times \sigma_{00_3} \times \sigma_{1_4} \times \sigma_{10_5} \times \sigma_{2_6} \times \sigma_{20_7} \times \sigma_{eoc_8}$) そして，Data.1 と Aggregate 署名 σ_a をユーザに送信する．

  ユーザ側：得られた画像データと Aggregate 署名 σ_a を著作者の秘密鍵で検証する．このとき，ハッシュ値は図 3 のように，個別データから生成する．
  そして，$e(\sigma_a, g_2) = e\left(\prod_{i=1}^{8} h_i, v\right)$ が成り立っているかを検証する．

- 追加データの通信時.
  サーバ側：送信されるそれぞれの署名と各データに対して同じ番号を割り振る．そして送信されるデータに該当する個別署名を集約し Aggregate 署名 σ_b を生成する．($\sigma_b \leftarrow \sigma_{01_9} \times \sigma_{11_{10}}$) そして，Data.2 と Aggregate 署名 σ_b をユーザに送信する．

  ユーザ側：得られた画像データと Aggregate 署名 σ_b を著作者の秘密鍵で検証する．そして，$e(\sigma_b, g_2) = e\left(\prod_{i=9}^{10} h_i, v\right)$ が成り立っているかを検証する．

最後に，通信終了後にユーザ側で受け取っている Data.1 と σ_a，Data.2 と σ_b，それぞれのペアに対して同じ番号を割り振る．番号の割り振られた σ_a，σ_b から Aggregate 署名 σ_c を生成する．($\sigma_c = \sigma_{a_1} \times \sigma_{b_2}$) 次に，Aggregate 署名 σ_c と得た画像データ全てを著作者の公開鍵でもう 1 度検証し，得た画像が著作者のものであるかを検証する．1 回の σ_c の検証により改めて要求した画像の正真性を検証することができる．検証が成功すれば，要求した画像は確かに著作者のものであるとユーザは確認できる．

表 1: JPEG 2000 符号列における Packet 数

	Size [byte]	Packet 数
圧縮処理： プレシンクトあり		
タイル:9 個，レイヤ:4	58108	3664
タイル:9 個，レイヤ:3	49847	2748
タイル:9 個，レイヤ:2	32971	1832
タイル:9 個，レイヤ:1	32916	916
圧縮処理： プレシンクトなし		
タイル:9 個，レイヤ:4	32935	862
タイル:9 個，レイヤ:3	32924	648
タイル:9 個，レイヤ:2	32908	432
タイル:9 個，レイヤ:1	32932	216

標準画像 lenna (ビットマップ，512×512，full-color).

4.3 性能評価

ここでは，提案方式に関する性能評価を行う．JPEG 2000 の符号列にある Packet の個数を Kakadu [6] を用いて計算した．表 1 は，標準画像 lenna を JPEG 2000 形式に圧縮し，Packet 数を調べた結果である．表 1 からわかるように，圧縮処理の方法によって異なるが，JPEG 2000 にはかなり多くの Packet が存在する．

また，PBC library [7] を用いて，提案方式を実装した．表 2 では提案方式における署名生成，個別署名の集約，検証での処理時間を示している．そして，表 2 より提案方式は署名生成処理に時間がかかることがわかる．しかし，JPIP はユーザ - サーバ間で行われ，署名生成は JPIP 処理の前に必要とされる．さらに，提案方式における集約，検証処理はサーバ，ユーザのそれぞれに負荷をかけないことが表 2 よりわかる．よって，実際の JPIP を想定した場合，提案方式は有効ではないかと考えられる．

5 まとめ

本稿では JPEG 2000 画像通信の国際標準である JPIP より得られる JPEG 2000 画像に対して，Aggregate 署名を用いて画像認証システ

表 2: 提案方式における各処理時間

	Server		User
処理データ数	署名時間 [s]	集約時間 [s]	検証時間 [s]
100	0.16	0.001	0.126
500	0.78	0.004	0.151
1000	1.53	0.007	0.182
1500	2.23	0.010	0.216
2000	3.01	0.014	0.242
2500	3.77	0.018	0.271
3000	4.48	0.021	0.303
3500	5.35	0.024	0.338
4000	6.05	0.027	0.362

Test machine– CPU: Intel(R) Core(TM)2 Duo P8600 2.40GHz, Memory: 512MB, gcc: version 4.2.4

ムを提案した．JPEG 2000 符号列は，数多くの Packet から構成されている．提案方式では，各 Packet から個別署名を取るため，サーバはかなりの計算量を個別署名生成時に必要とすることがわかった．しかし，それは JPIP 通信の前に必要とされることであり，JPIP 通信時に個別署名を集約することはサーバに対してそれほど負荷はない．今後の課題としては，データ量を削減できる個別署名の取り方と，Packet が改ざんされた際にその Packet を発見することが挙げられる．

参考文献

[1] “ Information technology -JPEG 2000 image coding system-part1: Core coding system, ” Int. Std. ISO/IEC IS-15444-1, 2000.

[2] “ Information technology -JPEG 2000 image coding system-part9: Interactivity tools, APIs and protocols, ” Int. Std. ISO/IEC IS-15444-9, 2000.

[3] J. Hara,“An implementation of JPEG 2000 interactive image communication system, ” ISCAS 2005, Vol.6, pp.5992–5925, May 2005.

[4] D. Boneh, C. Gentry, B. Lynn, H. Shacham, “ Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, ” EUROCRYPT 2003, LNCS2656, pp.416–432, 2003.

[5] D. Boneh, B. Lynn, and H. Shacham, “ Short signatures from the Weil pairing, ” Asiacrypt 2001, LNCS 2248, pp.514–532, Springer-Verlag, Berlin, 2001.

[6] D. Taubman, “ Kakadu Survey Documentation, ” 2005. `http://www.kakadusoftware.com/`.

[7] B. Lynn, “ PBC Library Manual 0.4.19, ” 2007. `http://crypto.stanford.edu/pbc/`.